XML Based Adaptive IPSec Security Policy Management in a Trust Management Context

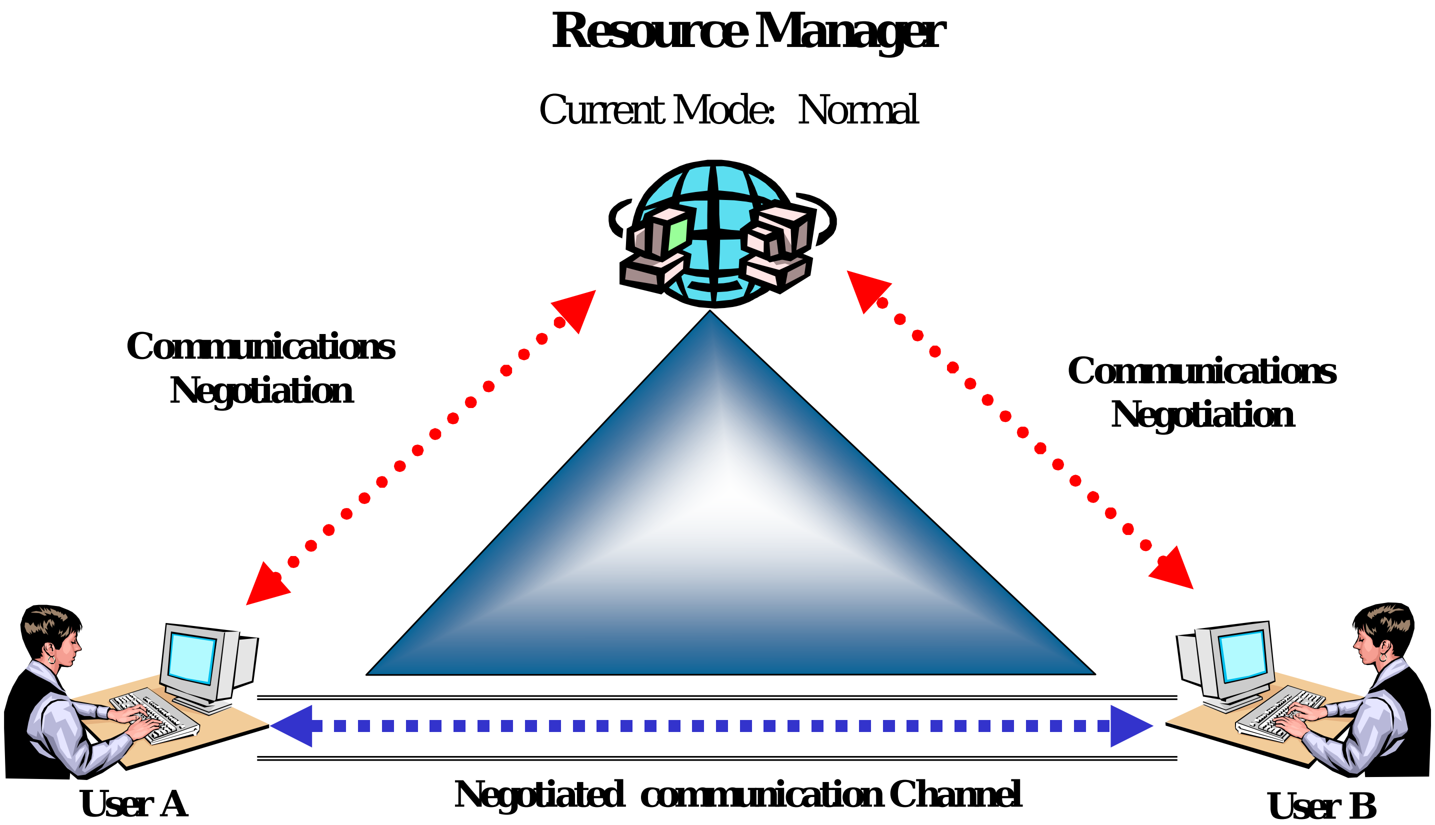
Raj Mohan

Jason Schwartz

Presentation Outline

- Background
- Disadvantages of current system
- Proposed XML-based architecture
- Application Demonstration

Quality of Security Service (QOSS)



Resource Manager

Current Mode: Normal

Communications Negotiation

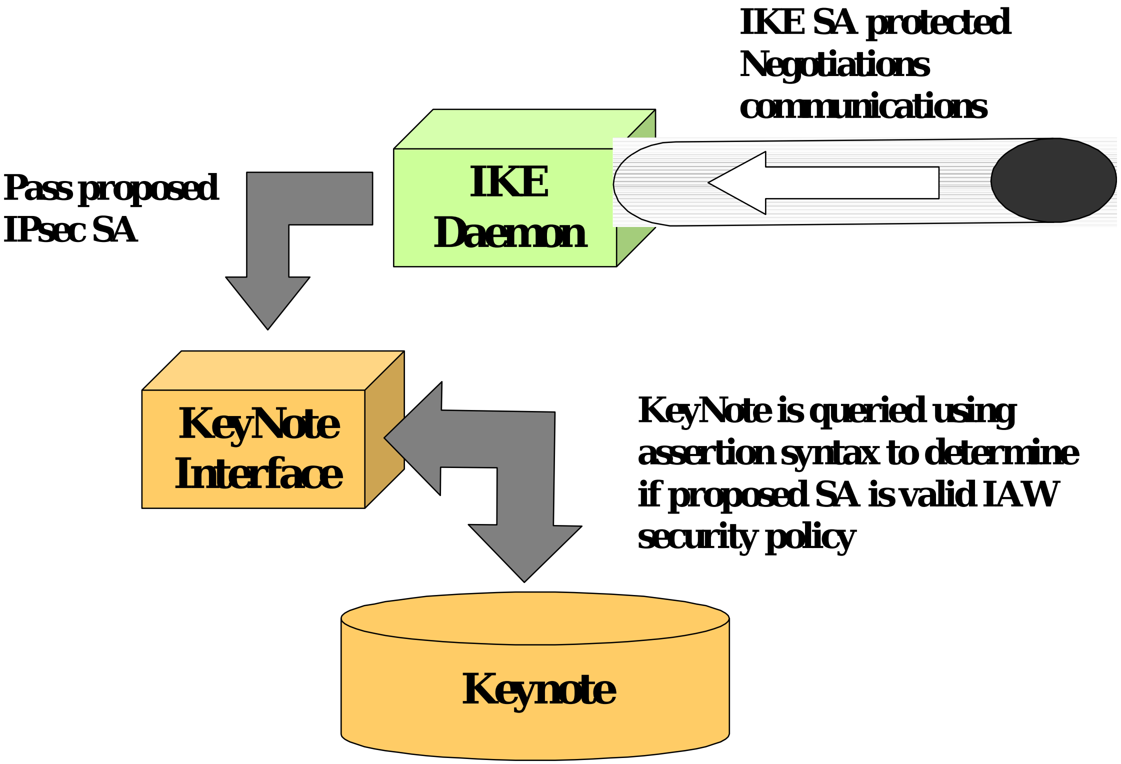
Communications Negotiation

User A

Negotiated communication Channel

User B

KeyNote Process



IKE SA protected
Negotiations
communications

IKE
Daemon

Pass proposed
IPsec SA

KeyNote
Interface

KeyNote is queried using
assertion syntax to determine
if proposed SA is valid IAW
security policy

Keynote

KeyNote Trust Management System

- Specified by RFC 2704
- Integrated into OpenBSD
- Mathematically proven syntax for assertion verification

KeyNote Policy Assertion Syntax

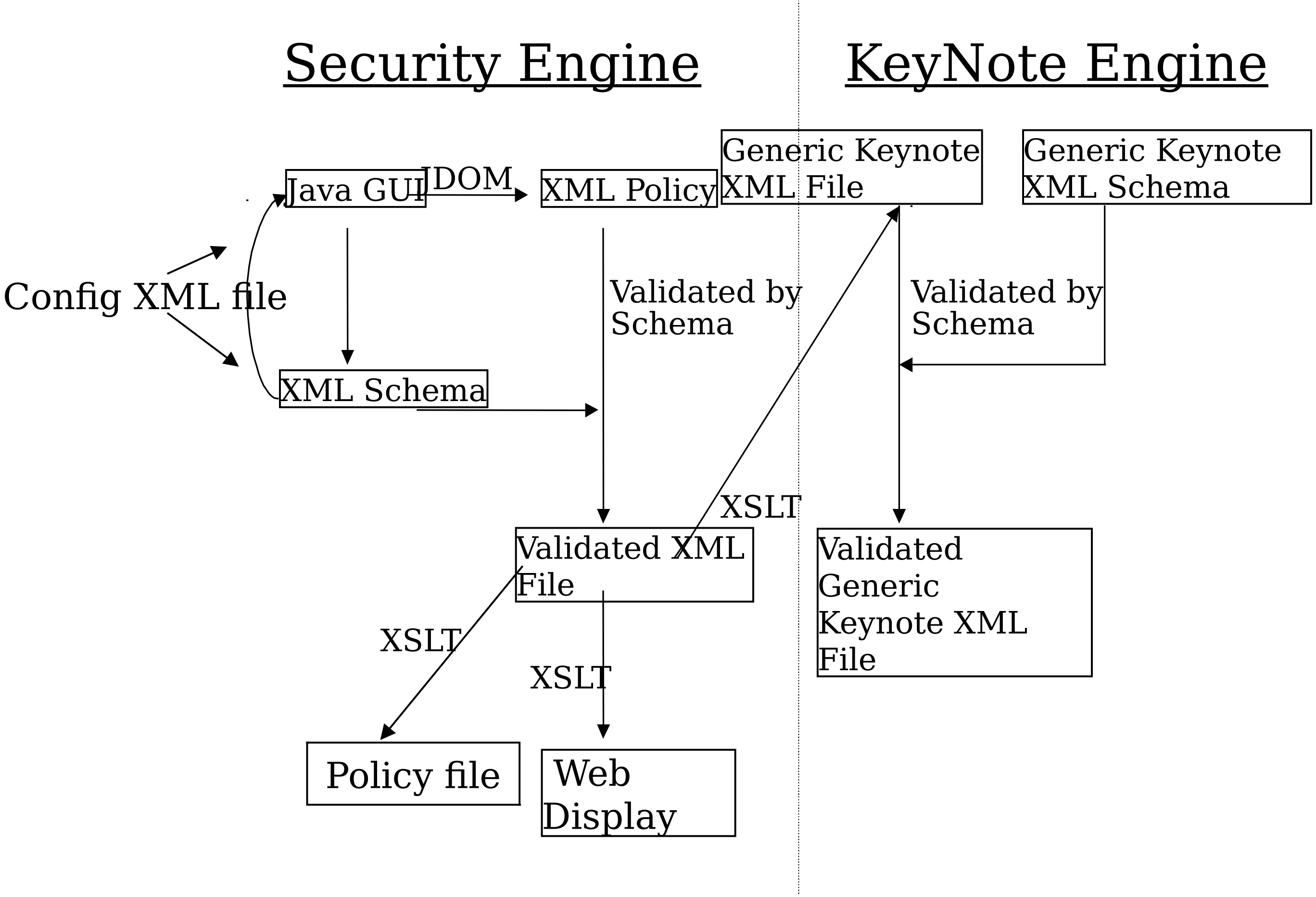
```
    KeyNote-Version: 2
    Authorizer: "POLICY"
    Licensees: "passphrase:mekmitasdigoat"
    Conditions: app_domain == "IPsec policy" &&
     ((esp_present == "yes") && (esp_encapsulation ==
“tunnel”) &&
          ((local_filter_port == "23") ||
            (remote_filter_port == "23")) &&
           (esp_enc_alg == "aes")) ||
      ((ah_present == "yes") && (ah_encapsulation ==
“tunnel”) &&
          ((local_filter_port == "79") ||
            (remote_filter_port == "79")) &&
           (ah_auth_alg == "hmac-sha"))
```

```
((((((((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "3des")) && (esp_present == "yes")) && (security_level
== "high")) && (network_mode == "normal")) && (app_domain == "IPsec policy")) || (((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-
sha")) && (esp_enc_alg == "3des")) && (esp_present == "yes")) && (security_level == "high")) && (network_mode == "normal")) && (app_domain ==
"IPsec policy"))) || (((((((local_filter_port == "79") && (ah_auth_alg == "hmac-sha")) && (ah_present == "yes")) && (security_level == "high")) &&
(network_mode == "normal")) && (app_domain == "IPsec policy")) || ((((((remote_filter_port == "79") && (ah_auth_alg == "hmac-sha")) && (ah_present
== "yes")) && (security_level == "high")) && (network_mode == "normal")) && (app_domain == "IPsec policy")))) || (((((((((local_filter_port ==
"23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "cast")) && (esp_present == "yes")) && (security_level == "medium")) && (network_mode ==
"normal")) && (app_domain == "IPsec policy")) || (((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "cast")) &&
(esp_present == "yes")) && (security_level == "medium")) && (network_mode == "normal")) && (app_domain == "IPsec policy"))) ||
(((((((local_filter_port == "79") && (ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) && (security_level == "medium")) && (network_mode ==
"normal")) && (app_domain == "IPsec policy")) || ((((((remote_filter_port == "79") && (ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) &&
(security_level == "medium")) && (network_mode == "normal")) && (app_domain == "IPsec policy"))))) || (((((((((local_filter_port == "23") &&
(esp_auth_alg == "hmac-md5")) && (esp_enc_alg == "des")) && (esp_present == "yes")) && (security_level == "low")) && (network_mode == "normal")) &&
(app_domain == "IPsec policy")) || (((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-md5")) && (esp_enc_alg == "des")) && (esp_present
== "yes")) && (security_level == "low")) && (network_mode == "normal")) && (app_domain == "IPsec policy"))) || (((((((local_filter_port == "79") &&
(ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) && (security_level == "low")) && (network_mode == "normal")) && (app_domain == "IPsec
policy")) || ((((((remote_filter_port == "79") && (ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) && (security_level == "low")) &&
(network_mode == "normal")) && (app_domain == "IPsec policy"))))) || (((((((local_filter_port == "23") && (esp_present == "yes")) && (esp_enc_alg
== "des")) && (esp_auth_alg == "hmac-md5")) && ((network_mode == "default") && (security_level == "default"))) || (((((remote_filter_port == "23")
&& (esp_present == "yes")) && (esp_enc_alg == "des")) && (esp_auth_alg == "hmac-md5")) && ((network_mode == "default") && (security_level ==
"default")))) || (((((local_filter_port == "79") && (ah_present == "yes")) && (ah_auth_alg == "hmac-md5")) && ((network_mode == "default") &&
(security_level == "default"))) || ((((remote_filter_port == "79") && (ah_present == "yes")) && (ah_auth_alg == "hmac-md5")) && ((network_mode ==
"default") && (security_level == "default")))))) || ((((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-md5")) && (esp_enc_alg ==
"blowfish")) && (esp_present == "yes")) && (security_level == "high")) && (network_mode == "impacted")) || ((((((remote_filter_port == "23") &&
(esp_auth_alg == "hmac-md5")) && (esp_enc_alg == "blowfish")) && (esp_present == "yes")) && (security_level == "high")) && (network_mode ==
"impacted"))) || ((((((local_filter_port == "79") && (ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) && (security_level == "high")) &&
(network_mode == "impacted")) || (((((remote_filter_port == "79") && (ah_auth_alg == "hmac-md5")) && (ah_present == "yes")) && (security_level ==
"high")) && (network_mode == "impacted")))) || ((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-md5")) && (esp_enc_alg == "cast")) &&
(esp_present == "yes")) && (security_level == "medium")) && (network_mode == "impacted")) || ((((((remote_filter_port == "23") && (esp_auth_alg ==
"hmac-md5")) && (esp_enc_alg == "cast")) && (esp_present == "yes")) && (security_level == "medium")) && (network_mode == "impacted"))) ||
((((((local_filter_port == "79") && (ah_auth_alg == "hmac-ripemd")) && (ah_present == "yes")) && (security_level == "medium")) && (network_mode ==
"impacted")) || (((((remote_filter_port == "79") && (ah_auth_alg == "hmac-ripemd")) && (ah_present == "yes")) && (security_level == "medium")) &&
(network_mode == "impacted"))))) || ((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-md5")) && (esp_enc_alg == "des")) && (esp_present
== "yes")) && (security_level == "low")) && (network_mode == "impacted")) || ((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-md5")) &&
(esp_enc_alg == "des")) && (esp_present == "yes")) && (security_level == "low")) && (network_mode == "impacted"))) || ((((((local_filter_port ==
"79") && (ah_auth_alg == "hmac-ripemd")) && (ah_present == "yes")) && (security_level == "low")) && (network_mode == "impacted")) ||
(((((remote_filter_port == "79") && (ah_auth_alg == "hmac-ripemd")) && (ah_present == "yes")) && (security_level == "low")) && (network_mode ==
"impacted")))))) || ((((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "aes")) && (esp_present == "yes")) &&
(security_level == "high")) && (network_mode == "crisis")) || ((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg ==
"aes")) && (esp_present == "yes")) && (security_level == "high")) && (network_mode == "crisis"))) || ((((((local_filter_port == "79") &&
(ah_auth_alg == "hmac-sha")) && (ah_present == "yes")) && (security_level == "high")) && (network_mode == "crisis")) || (((((remote_filter_port ==
"79") && (ah_auth_alg == "hmac-sha")) && (ah_present == "yes")) && (security_level == "high")) && (network_mode == "crisis")))) ||
((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "3des")) && (esp_present == "yes")) && (security_level ==
"medium")) && (network_mode == "crisis")) || ((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "3des")) &&
(esp_present == "yes")) && (security_level == "medium")) && (network_mode == "crisis"))) || ((((((local_filter_port == "79") && (ah_auth_alg ==
"hmac-sha")) && (ah_present == "yes")) && (security_level == "medium")) && (network_mode == "crisis")) || (((((remote_filter_port == "79") &&
(ah_auth_alg == "hmac-sha")) && (ah_present == "yes")) && (security_level == "medium")) && (network_mode == "crisis"))))) ||
((((((((local_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "3des")) && (esp_present == "yes")) && (security_level ==
"low")) && (network_mode == "crisis")) || ((((((remote_filter_port == "23") && (esp_auth_alg == "hmac-sha")) && (esp_enc_alg == "3des")) &&
(esp_present == "yes")) && (security_level == "low")) && (network_mode == "crisis"))) || ((((((local_filter_port == "79") && (ah_auth_alg == "hmac-
ripemd")) && (ah_present == "yes")) && (security_level == "low")) && (network_mode == "crisis")) || (((((remote_filter_port == "79") &&
(ah_auth_alg == "hmac-ripemd")) && (ah_present == "yes")) && (security_level == "low")) && (network_mode == "crisis"))))))
```

Drawbacks of Current System

- Impractical to manually create and edit an actual policy file
- Policy edits may introduce security inconsistencies
- Policy file not self-describing
- Cannot extract pertinent security status information

XML Based System Architecture



Conclusion

- XML & Java architecture to the rescue
  - Provides GUI interface for creating and editing policy file
  - GUI is dynamic based on XML file
  - Prevents user-introduced inconsistencies using schema validation
  - Ability to extract information from policy file
  - Ability to display policy file in a human-readable form
  - Backward compatible with old system

Questions ?